

Enrollment No./Seat No.:

GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering - SEMESTER - IV EXAMINATION - SUMMER 2025

Subject Code: 3144803

Date: 19-05-2025

Subject Name: Number Theory

Time: 10:30 AM TO 01:00 PM

Total Marks: 70

Instructions

1. Attempt all questions.
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.
4. Simple and non-programmable scientific calculators are allowed.

	Marks
Q.1 (a) Find the GCD of (12378, 3054) using Euclid's Algorithm.	03
(b) (i) What is The Goldbach Conjecture? Explain with an example. (ii) What is a set of 2025 consecutive integers none of which are prime.	04
(c) Determine all solutions in the positive integers of the following Diophantine equation $172x + 20y = 1000$.	07
Q.2 (a) Solve linear congruence $18x \equiv 30 \pmod{42}$ and find the other incongruent solutions.	03
(b) State Wilson's Theorem and find the remainder when $2(26!)$ is divided by 29.	04
(c) State Chinese Remainder theorem and find the value of x for the given set of congruent equations using Chinese Remainder theorem. $x \equiv 2 \pmod{3}$ $x \equiv 3 \pmod{5}$ $x \equiv 2 \pmod{7}$	07

OR

(c) Solve the system of linear congruences $x \equiv 1 \pmod{4}$ $x \equiv 2 \pmod{3}$ $x \equiv 3 \pmod{5}$	07
Q.3 (a) Find the highest power of 2 which divides $25!$	03
(b) Calculate $\tau(2700)$ and $\sigma(2700)$.	04
(c) Write down Mobius inversion formula and find the $\mu(6)$, $\mu(7)$ and $\mu(100)$.	07

OR

(a) Calculate $\phi(360)$, $\phi(6615)$ and $\phi(9952)$.	03
(b) State Euler's Theorem and evaluate $2^{100000} \pmod{77}$.	04

- (c) Given $n \geq 1$, let $\sigma_s(n)$ denote the sum of the s^{th} powers of the positive divisors of n ; that is,

$$\sigma_s(n) = \sum_{d|n} d^s$$
 Verify the following:
 (a) $\sigma_0 = \tau$ and $\sigma_1 = \sigma$.
 (b) σ_s is a multiplicative function.

- Q.4** (a) Find all primitive root of 17. 03
 (b) Define Euler's solvability criterion with one example. 04
 (c) Solve $x^2 \equiv 23 \pmod{7^2}$. 07

OR

- (a) Evaluate Legendre Symbol : $(29/53)$ and $(19/23)$. 03
 (b) What is Jacobi symbol? State its properties. 04
 (c) Solve $4x^9 \equiv 7 \pmod{13}$. 07

- Q.5** (a) Explain Symmetric key Encryption with Public Key. 03
 (b) If the Caesar cipher produced "ZCQR MD JSAT" what is the plain text message? 04
 (c) P and Q are two prime numbers. $P = 11$ and $Q = 31$. Take public key $E = 7$. If the plain text value is 25, then what will be the cipher text value according to the RSA algorithm? 07

OR

- (a) Explain Asymmetric key Encryption with Private Key. 03
 (b) Explain Knapsack Cryptosystem. 04
 (c) For $p = 13$ and $q = 23$ and choose $d = 47$. Apply RSA algorithm where Cipher message is 157 and thus find the plain text. 07
